Exhibit 80

Excerpts of SW-SEC00522109

From: Houston, Eric [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=4CAE54BEB3C049C59BEF872FCF73FFFD-HOUSTON, ER]
Sent: 1/12/2021 5:26:08 PM
To: Cline, Brad [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=c1da7afa0bce413f9c32ce66040660f3-Cline, Brad]
Subject: RE: Corporate Network Security Recommendations
Attachments: Security Assessment.pptx

Flag: Follow Up

Brad

After our discussion yesterday, I conducted a discovery session with the team about the Palo Alto Firewall + VPN. Matching them against the best practices in my presentation.
Below are the points that could be addressed: Lets discuss the risk vs benefits and impact when you have a minute.

VPN

- Split-tunneling is allowed, we should consider disabling forcing all traffic via the tunnel and disabling local routing. ***{configuration}***
    - Risk: local LAN can use vpn-client as a router to access SolarWinds

Firewall

- Logging is not retained ***{configuration}***
    - Risk: no historical information is available outside of information forwarded to SIEM after log rotation. Recommend 2yr retention offsite
- Rules should be reviewed from DEV to TUL ***{operational}***
    - Risk: any high risk area, DMZ, Partner zone, or in this case LAB/SW development traffic should initiate only from TUL to this environment, not the other way around.
- Rules should be linked to request (ticket with user requestor, machine owner) and have a two year expiration/review ***{operational}***
    - Risk: old or expired rules, linked to resources or people that are no longer valid.
- Issues with user identification – not always reliable, configuration problem ***{configuration}***
    - Risk: unable to configure rules that apply to user or potentially associate traffic with a user. Additionally internet traffic is allowed without this validation
- Administration/Hardening – Policy – ***{operational}***
    - Risk: Firewalls are accessible from Public, internet – however limited via ACL to only SolarWinds IP
    - Risk: Vendor patches/releases should be review and implemented more often.

Improvements: (we will engage, the VAR and Vendor on specifics listed below + any additional capabilities)

- HIP check capabilities
    - Team suggests that we do not own the licensing to perform these operations – will validate with account team at Palo Alto
    - What are we looking to validate – and acceptance level before remediation/access restriction
        - OS version
        - Windows update on and Patch level
        - Antivirus installed, turned on and up to date
        - EDR client – Falcon installed?
    - Prove SolarWinds asset
        - Via machine certificate, installed

- What about local administrative rights – certificate exporting
- What about contractors/vendors – BYOD policy if any

- SSL inspection – better visibility into packets
- DNS outbound validation, - like umbrella

Regards,

Eric Houston | IT Manager

solarwinds

Office: +1.512.498.6121
Mobile +1 512.516.1302
Eric.Houston@Solarwinds.com

Solarwinds US, Inc. | 7171 Southwest Parkway, Building 400, Austin, TX 78735

From: Houston, Eric
Sent: Monday, January 11, 2021 4:38 PM
To: Cline, Brad <brad.cline@solarwinds.com>
Subject: Corporate Network Security Recommendations

Hi Brad

You had asked that I review the infrastructure for design and security best practices and make recommendations. Since I still need to understand the architecture a bit more in detail, I instead put down my thoughts as it comes to at least security.

Attached is nothing more than a collection of thoughts, in regards to my experience with best practices. I have not validated if SolarWinds adheres to any of these nor have I seen a written security policy yet for the organization. I figured I could review this with everybody and develop one for IT after validating and making changes where we decide together.

Other points:

In regards to the SNMP, I think you heard this morning that Najrani addressed this task already for Network and UC still needs to do so.

As you and I spoke today, I will start working on understand the capabilities with Palo short, term and work on a 3-6mo plan for NAC corporate wide long term.

There does not seem to be a single source of truth in regards to documentation/assets/configuration etc. so I would like to make this a task moving forward once the dust settles.

Regards,

Eric Houston | IT Manager

solarwinds

Office: +1.512.498.6121
Mobile +1 512.516.1302

Eric.Houston@Solarwinds.com

Solarwinds US, Inc. | 7171 Southwest Parkway, Building 400, Austin, TX 78735

SolarWinds

Corporate Network Security Recommendations

Eric Houston – IT Manager

Internal LAN Network

- SolarWinds official corporate devices (workstations, laptops, network devices) can be connect to wired LAN without specific authorization.
  - All other devices should be forbidden. No BYOD policy, unless we have Endpoint and Mobility Management.
- Internally connected devices should not provide network services, for instance DHCP/DNS etc. These should be in the Services zone.
- NAC – Network Access Control, should be implemented – minimum DHCP filtering as a starting point
  - Posturing and validation of software, up to date prior to access else quarantine

VPN

- Virtual Private Networks are an extension of SolarWinds, only corporate approved devices should be allowed VPN connection
- Site to Site
  - IPSEC over internet bypassing internal firewall should only be allowed for trusted Branch office connections and can terminate to WAN/LAN zone
  - New company integration should be connected with limited – needed only access after security team approves
  - Partners VPN – should be reviewed thoroughly and not connected directly to the LAN but a specific partners zone (like DMZ) that limits access
- User VPN
  - Should use two factor authentication
  - Client should be patched current, or at very least automatic update turned on
  - Corporate antivirus up and running
  - Should be recognized on SolarWinds Active Directory
  - Should not allow split-tunneling on VPN
  - Connection should not remain open and turned on for more that 12 hours without re-authentication
- Non SolarWinds access for VPN
  - Should have only limited access to needed resources – in specific secured zone
  - Account should have Lifecyle management (when contractor leaves, account is disabled)
- Outgoing VPN connections
  - Connections can be allowed as long as the connecting machine is not accessible to/from the SolarWinds network while connected (no spit – tunneling)

Other areas of Security

- Infrastructure
  - Making sure all hardware (including network/UC) are patch current and recommend design best practices are in place – vulnerabilities removed – vendor recommended hardening
  - Administrative access should have AAA
  - No single admin should have all access – role based suggested
  - MFA or Bastion suggested to remove privileged access account usage
  - Micro segmentation within the VLAN Host to Host - NSX/ACI
- Email:
  - inbound anti-spam + anti-malware
  - No email forwarding
  - Email from only corporate devices or authenticated with MFA
  - Identification on Email of External sources